International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Multiple Keyword Search for Encrypted Cloud Storage

Revathi. S[1], Subalaxmi. M[2], Vishnupriya. S[3], Ranjeeth Kumar. C[4]

[1,2,3]Student, Dept. of Information Technology, Sri Ramakrishna Engineering College, Tamilnadu, India
[4]Assistant Professor (Sr. Grade), Dept. of Information Technology, Sri Ramakrishna Engineering College, Tamilnadu, India

---

Abstract - *Cloud computing is a technology, which provides low cost, scalable computational capacity. The storage and access of confidential documents have been identified as one of the central problems in this area. While many schemes have been proposed to perform conjunctive keyword search, less attention has been noted. In this paper, we proposed a phrase search technique based on bloom-filters which is faster than existing system, with better storage and communication cost. Our technique uses a series of n-gram filters and conjunctive keyword search to support the functionalities. This approach also described the false positive rate.*

***Key Words*: Phrase Search, Conjunctive Keyword Search, Bloom Filters, False Positive Rate, Hashing**

1. INTRODUCTION

Cloud computing has generated much interest in the research community in recent years. As organizations and individuals adopt cloud technologies, many have become aware of the serious concerns regarding security and privacy of accessing personal and confidential information over the Internet.

To search over encrypted documents stored on cloud, many schemes has been proposed but less attention have been noted on more search techniques. To overcome the storage and access of confidential documents stored in cloud, we proposed a phrase search scheme using bloom filters which achieves a much faster response time than existing solutions. This approach also described the false positive rate for the keyword search.

2. PROBLEM DESCRIPTION

System framework: In this framework, we designed a standard keyword search protocol. During setup, the data owner generates the required encryption keys for hashing and encryption operations. Then, all documents in the database are parsed for keywords. Bloom filters tied to hashed keywords and n-grams are attached. The documents are then symmetrically encrypted and uploaded to the cloud server. To add files to the database, the data owner parses the files as in setup and uploads them with Bloom filters attached to the cloud server. To remove a file from the data, the data owner simply sends the request to the cloud server, who removes the file along with the attached Bloom filters. To perform a search, the data user enters keyword then it computes and sends a trapdoor encryption of the queried keywords to the cloud to initiate a protocol and returns accurate file.

Here we implement some modules. They are Home, Data Owner, Data User and Cloud Storage.

Data Owner: In Data Owner module, Initially Data Owner must have to register their detail and after login he/she has to verify their login through OTP. Then data Owner can upload files into cloud server with encrypted keywords and hashing algorithms. He/she can view the files that are uploaded in cloud. Data Owner can approve orejecthfile request sent by data users.

Data User: In Data User module, Initially Data Users must have to register their detail and then login into cloud. Data Users can search all the files upload by data owners. He/she can send request to the files and then request will send to the data owners. If data owner approve the request then he/she will receive the decryption key in registered

Cloud Storage: This module completely shows the accurate data stored in the cloud storage. Thus helps users search the files needed. Cloud Provider can view all the Data owners and data users' details and also the files uploaded by the data owners.

3. RELATED TECHNOLOGY

3.1 Java:

Java is a general-purpose computer-programming language that is concurrent, class-based, object -oriented and specifically designed to have as few implementation dependencies as possible. It is intended to let application developers "write once, run anywhere" (WORA), meaning that compiled Java code can run on all platforms that support Java without the need for recompilation.

3.2 MySQL Database

MySQL is the most widely-used open source SQL database management system, is developed, distributed, and supported by Oracle Corporation. Database Management System such as MySQL server is needed in order to add, access, and maintain data stored in a database which is a structured collection of data.

4. METHODOLOGY

In this approach we used three methodology which is used to retrieve data from cloud fast and secure. The algorithm and protocol is used to encrypt the files and keyword and took the value for all keywords and file to decrypt file faster stored in the cloud server. Here we using an real time cloud Drive HQ to store document

•AESALGORITHM
•DESALGORITHM
• HASHING

The MySQL server is used for storing the data in this application. The details of the data admin and data user are stored in the database. Each admin and user will have unique email id to login to the application. The data may include details like name, address, username, password, date of birth, photo etc. The uploaded files are stored in the database.

There are 4 modules namely

- HOME.
- DATA OWNER MODULE.
- DATA USER MODULE.
- CLOUD STORAGE.

4.1 DATA OWNER MODULE

a) Registration Module:

Registration module is used for admin authentication purpose in which administrator can only access this admin module. It contains authentication type and personal details of admin such as name, designation, mail id, phone number, address, username, password, date of birth, photo and also it can be stored and maintained in database. The person who is authenticating it will access it by using username and password.

b) Login Module:

This module checks the admin register page by checking with mail id and password which is already stored in database. It true data is authenticated that allows to go for main admin module or otherwise that will stay in current page by showing up alert message as Invalid User.

Fig -4.1.1: Data Owner Login

Fig -4.1.2: Login OTP Verification

c) Home Module:

In this module Data Owner Home this contains Basic functionalities of cloud that can be helpful for data Owner who is logged on already in session.

Fig -4.1.3: Data Owner Home

d) Upload Module:

In which, the files are uploaded in format of file name, keywords. In this case single keyword does not helps in the searching to avoid this we are using three types of keyword to fetch the file. The file are stored in the encrypted formats.

Fig -4.1.4: Upload Module

e) My Files Module:

My Files page shows files which is uploaded by particular data user.

Fig -4.1.5: My Files Module

f) Approvals Module:

In this module, the request send by the data user can be authenticated by the data owner. Either accepts the request or rejects the request.

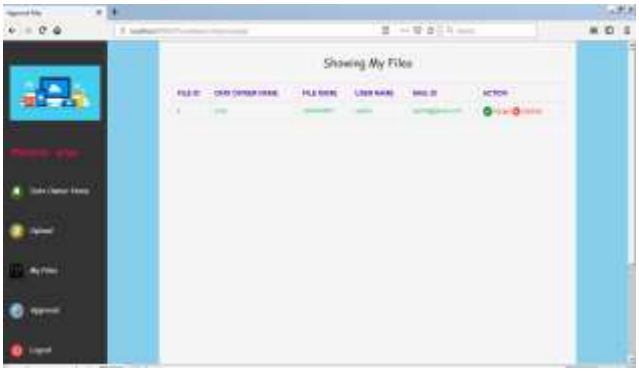


Fig -4.1.6: Approval Module

g) Logout:

This module which completely moves you out from the data owner session to the home session.

4.2 DATA USER MODULE:

a) Registration Module:

Registration module is used for data user authentication purpose in which administrator can only access this admin module. It contains authentication type and personal details of admin such as name, designation, mail id, phone number, address, username, and password, date of birth, photo and also it can be stored and maintained in database. The person who is authenticating it will access it by using username and password.

Fig -4.2.1Data Owner Signup

b) Login Module:

This module checks the admin register page by checking with mail id and password which is already stored in database. It true data is authenticated that allows to go for main admin module or otherwise that will stay in current page by showing up alert message as Invalid User.

Fig -4.2.2 Login Module

c) Home Module:

In this module Data user Home this contains Basic functionalities of cloud that can be helpful for data Owner who is logged on already in session.

Fig -4.2.3 Home Module

d) Search:

Search module, in which you can search the file that you want. The search request is send as query that finds the data from the cloud and shows your approximate search, you can send request to the file so that particular data owner either accept/decline request as their wish.

Fig -4.2.4 Search Module

e) Requested files:

This shows your file is either accepted or not. If accepted you can view file by particular generated decryption key so that encrypted file will be downloaded as decrypted the readable format.

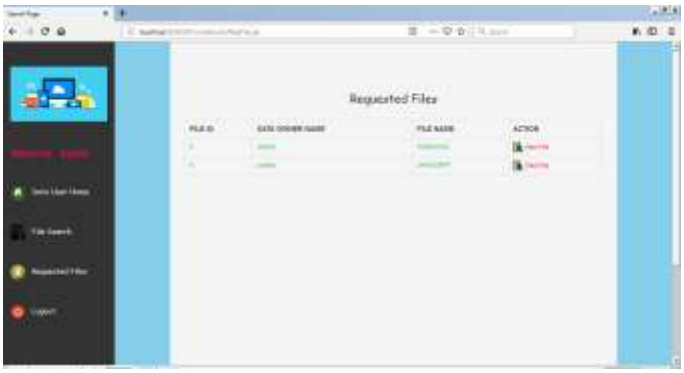
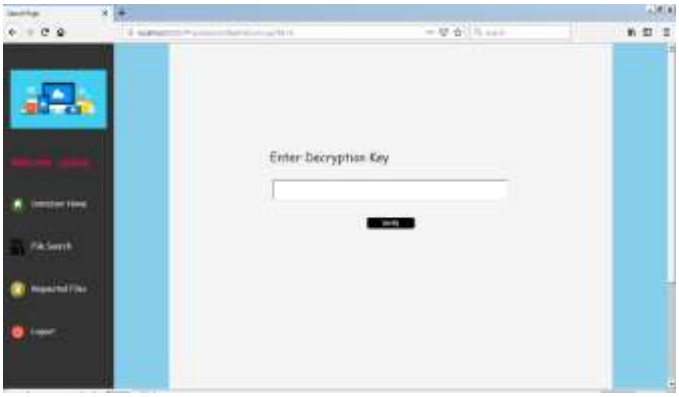
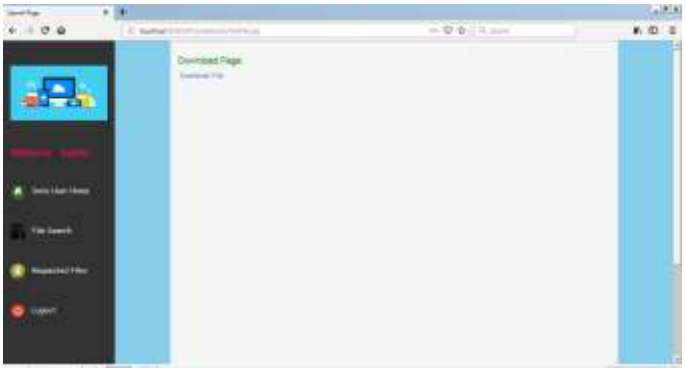


Fig -4.2.5 Requested Files





g) Logout:

This module which completely moves you out from the data user session to the home session.

4.3 CLOUD STORAGE MODULE:

This module completely shows the accurate data stored in the cloud storage .This help you search file that you needed.

Fig -4.3.1 Cloud Storage

5. ADVANTAGES AND DISADVANTAGES

5.1 Advantages:

• The scheme is scalable, where documents can easily be removed and added to the corpus.
• We also describe modifications to the scheme to lower storage cost at a small cost in response time and to defend against cloud providers with statistical knowledge on stored data.

5.2 Disadvantages:

Although the scheme employs phrase search technique, conjunctive keyword search method is also employed which was used in the existing system that consumed time.

6. CONCLUSION

In this paper, we presented a phrase search scheme based on Bloom filter that is significantly faster than Existing approaches, requiring only a single round of communication

and Bloom filter verifications. Our approach also effectively allows phrase search to run independently without first performing a conjunctive keyword search to identify candidate documents. It also achieves a lower storage cost than all existing solutions except where a higher computational cost was exchanged in favor of lower storage. While exhibiting similar communication cost to leading existing solutions, the proposed solution can also be adjusted to achieve maximum speed or high speed with a reasonable storage cost depending on the application.

7. REFERENCES

[1] K. Cai, C. Hong, M. Zhang, D. Feng, and Z.Lv, "A secure conjunctive keywords search over encrypted cloud data against inclusion-relation attack," in IEEE International Conference on Cloud Computing Technology and Science, 2013, pp. 339–346.
[2] Y. Yang, H. Lu, and J. Weng, "Multi-user private keyword search for cloud computing," in IEEE Third International Conference on Cloud Computing Technology and Science, 2011, pp. 264–271.
[3] F. Kerschbaum, "Secure conjunctive keyword searches for unstructured text," in International Conference on Network and System Security, 2011, pp. 285–289.
[4] C. Hu and P. Liu, "Public key encryption with ranked multikeyword search," in International Conference on Intelligent Networking and Collaborative Systems, 2013, pp. 109–113.
[5] Z. Fu, X. Sun, N. Linge, and L. Zhou, "Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query," IEEE Transactions on Consumer Electronics, vol. 60, pp. 164–172, 2014.
[6] M. Zheng and H. Zhou, "An efficient attack on a fuzzy keyword search scheme over encrypted data," in International Conference on High Performance Computing and Communications and Embedded and Ubiquitous Computi UIng, 2013, pp. 1647–1651.
[7] S. Zittrower and C. C. Zou, "Encrypted phrase searching in the cloud," in IEEE Global Communications Conference, 2012, pp. 764 – 770
[8] C. Liu, L. Zhu, L. Li, and Y. Tan, "Fuzzy keyword search on encrypted cloud storage data with small index," in 2011 IEEE International Conference on Cloud Computing and Intelligence Systems,2011,pp.269-273.

[9].P.F.Brown ,P.V. deSouza, R. L. Mercer, V. J. D. Pietra, and J. C. Lai, "Class-based n-gram models of natural language," Computational Linguistics, vol. 18, no. 4, pp. 467–479, 1992.
[10] D. Jurafsky and J. H. Martin, Speech and Language:An Introduction to Natural Language Processing, Speech Recognition, and Computational Linguistics. Prentice Hall, 2009.